CLAIMS

1. A tamper-resistant electronic circuit for implementation in a device, said tamper-resistant electronic circuit comprising:

- means for tamper-resistantly storing a secret not accessible over an external circuit interface;
- means for performing cryptographic processing at least partly in response to said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit during usage of said device; and
- means for performing a security-related operation in response to said internally confined device-specific security data.

2. The electronic circuit according to claim 1, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

3. The electronic circuit according to claim 1, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said device-specific security data.

4. The electronic circuit according to claim 3, wherein said operation is configured for generating a device-specific fingerprint embedded into said digital content.

5. The electronic circuit according to claim 1, wherein said means for performing cryptographic processing is configured for generating said device-specific security data provided that additional input data in the form of predetermined trigger data is applied over an external circuit interface during usage of said device, wherein said trigger data is defined during configuration of said device.

6. The electronic circuit according to claim 5, wherein said trigger data is defined in a configuration phase during manufacturing of said device.

7. The electronic circuit according to claim 5, wherein said trigger data is defined based on configurational device-specific security data provided during configuration of the device, and said electronic circuit further comprises:

- means for generating, based on said stored secret and said configurational device-specific security data, said trigger data as a cryptographic representation of said configurational device-specific security data during configuration of said device;
- means for outputting said cryptographic representation over an external circuit interface during configuration; and
- means for internally re-generating said device-specific security data during usage of said device provided that said additional input corresponds to said cryptographic representation.

8. The electronic circuit according to claim 7, wherein said configurational device-specific security data is provided over an external circuit interface.

9. The electronic circuit according to claim 7, further comprising means for internally generating, during configuration of said device, said configurational device-specific security data at least partly based on said stored secret.

10. The electronic circuit according to claim 9, wherein said means for internally generating said configurational device-specific security data comprises means for generating a private key at least partly based on said stored secret, and said trigger data is generated as a cryptographic representation of said private key during configuration of said device.

11. The electronic circuit according to claim 1, further comprising means for making, during configuration of said device, said device-specific security data available over an external circuit interface provided that a predetermined device access code is entered into the electronic circuit.

12. The electronic circuit according to claim 1, further comprising means for disabling internal access to at least one of said stored secret and said device-specific security data unless a predetermined device access code is entered into the electronic circuit.

13. The electronic circuit according to claim 11 or 12, further comprising:

- means for authentication of a manufacturer of said device;
- means for providing, during device manufacturing, said device access code to said device manufacturer in response to successful authentication.

14. The electronic circuit according to claim 13, wherein said device access code is provided as a challenge-response pair based on a challenge from said device manufacturer and said stored secret.

15. The electronic circuit according to claim 1, wherein said means for performing a security-related operation based on said confined device-specific security data comprises:

- means for performing additional cryptographic processing based on said device-specific security data and further external input data to generate further security data; and
- means for performing said security-related operation in response to said further security data.

16. The electronic circuit according to claim 15, wherein said device-specific security data represents a private key, and said further external input data represents an

encryption of said further device-specific security data by the corresponding public key.

17. The electronic circuit according to claim 16, wherein said further security data represents a symmetric content decryption key issued by a content provider, and said device-specific security data represents a private key of a device manufacturer.

18. The electronic circuit according to claim 1, wherein said means for performing cryptographic processing to generate device-specific security data is configured for generating a symmetric cryptographic key in response to a seed applied over an external circuit interface.

19. The electronic circuit according to claim 1, wherein said means for performing cryptographic processing to generate device-specific security data is configured for generating a private key at least partly based on said stored secret, and said means for performing a security-related operation comprises means for performing asymmetric cryptography operations based on said internally confined private key.

20. The electronic circuit according to claim 19, further comprising means for generating a public key corresponding to said private key during configuration of said device, and means for outputting said public key over an external circuit interface.

21. The electronic circuit according to claim 19, wherein the corresponding public key is generated in response to said secret and additional input data during configuration of the device, and said means for performing cryptographic processing to generate said private key is operable for internally re-generating said private key provided that at least part of the same additional input data is applied over an external circuit interface during usage of the device.

22. The electronic circuit according to claim 19, further comprising:

- means for performing shared key generation to generate a new shared key based on said generated private key and a public key of an intended communication partner; and
- means for performing cryptographic processing based on said new shared key.

23. The electronic circuit according to claim 1, wherein multiple individual trigger data signals are defined during configuration of said device, each trigger data signal being associated with a respective individual device-specific security data, and said means for performing cryptographic processing is configured for generating a particular device-specific security data provided that the associated trigger data is applied over an external circuit interface during usage of said device.

24. The electronic circuit according to claim 23, wherein said electronic circuit is operable as a multi-user identity module, and said security-related operation includes authentication and key agreement.

25. The electronic circuit according to claim 23, wherein said electronic circuit is operable as a multi-channel decoder, and said security-related operation includes channel decoding.

26. The electronic circuit according to claim 1, wherein said means for cryptographic processing is operable for generating said device-specific security data as a chain of $k$ bind keys $B_1, \ldots, B_k$ in response to corresponding bind identities $R_1, \ldots, R_k$ according to the following formula:

$$B_i = f(B_{i-1}, R_i) \qquad \text{for } i=1, \ldots, k,$$

where $B_0$ represents the stored secret, and f is a cryptographic one-way function.

27. The electronic circuit according to claim 1, wherein said electronic circuit is an integrated circuit (IC).

28. A device implemented with a tamper-resistant electronic circuit, said electronic circuit comprising:

- means for tamper-resistantly storing a secret not accessible over an external circuit interface;
- means for performing cryptographic processing at least partly in response to said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit during usage of said device; and
- means for performing a security-related operation in response to said internally confined device-specific security data.

29. The device according to claim 28, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

30. The device according to claim 28, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said device-specific security data.

31. The device according to claim 28, wherein said means for performing cryptographic processing is configured for generating said device-specific security data provided that additional input data in the form of predetermined trigger data is applied over an external circuit interface of the electronic circuit during usage of said device, wherein said trigger data is defined during configuration of said device.

32. A method for management of security data for a device, said method comprising the steps of:

- storing, in a controlled environment during manufacturing of a tamper-resistant electronic circuit, a secret randomized number in said electronic circuit such that the secret number is not available outside of said electronic circuit;
- implementing, during circuit manufacturing, functionality into said electronic circuit for performing cryptographic processing at least partly based on said stored secret number to generate device-specific security data internally confined within said electronic circuit during usage of the device;
- implementing, during circuit manufacturing, a security-related operation into said electronic circuit, said security-related operation being configured for receiving at least said internally confined device-specific security data as input during usage of the device; and
- installing, during device manufacturing, said electronic circuit into said device.

33. The method according to claim 32, wherein said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication.

34. The method according to claim 32, wherein said device is configured for producing digital content and said security-related operation is configured for marking said digital content based on said device-specific security data.

35. The method according to claim 32, further comprising the step of providing, during configuration of the device, trigger data to be applied later during usage of the device in order to be able to generate said device-specific security data within said electronic circuit.

36. The method according to claim 35, further comprising the step of securely transferring said trigger data from a device configuring party to said device.

37. The method according to claim 35, further comprising the steps of:

- entering, in a controlled environment during device configuration, said trigger data as input data into said electronic circuit in order to obtain device-specific security data from the cryptographic functionality of the electronic circuit;
- recording, in a controlled environment during device configuration, said device-specific security data and said input data; and
- entering, in a controlled environment during device configuration, a predetermined device access code into the electronic circuit for accessing the device-specific security data over an external circuit interface.

38. The method according to claim 37, wherein said device-specific security data is usable by the configuring party or a trusted third party for security-related operations in relation to the device, said input data being required by the electronic circuit to internally regenerate the device-specific security data.

39. The method according to claim 35, further comprising the steps of:

- generating, in a controlled environment during device configuration, device-specific security data;
- entering, in a controlled environment during device configuration, said generated device-specific security data into said electronic circuit in order to obtain said trigger data as a result representation from the cryptographic functionality of the electronic circuit; and
- recording, in a controlled environment during device configuration, said result representation and the previously generated device-specific security data.

40. The method according to claim 39, wherein said device-specific security data is usable by the configuring party or a trusted third party for security-related operations in relation to the device, said result representation being required by the electronic circuit to internally regenerate the device-specific security data.

41. A method for maintaining data security in relation to network communication between a network device and an external communication partner, wherein said network device comprises a tamper-resistant electronic circuit with a stored secret not accessible outside of said electronic circuit, and said method comprises the steps of:

- performing, in said electronic circuit, cryptographic processing at least partly based on said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit; and
- performing, in said electronic circuit, an operation related to data security in network communication between said network device and said communication partner based on said internally confined device-specific security data.

42. The method according to claim 41, wherein said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation.

43. The method according to claim 41, further comprising the step of applying predetermined trigger data over an external circuit interface of said electronic circuit during usage of the network device in order to be able to internally generate said device-specific security data, wherein said predetermined trigger data is defined during configuration of said network device.

44. The method according to claim 43, wherein said trigger data is defined in a configuration phase during manufacturing of the network device.

45. A method for marking digital content produced by a content-producing device, wherein said content-producing device comprises a tamper-resistant electronic circuit with a stored secret not accessible outside of said electronic circuit, and said method comprises the steps of:

- performing, in said electronic circuit, cryptographic processing at least partly based on said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit; and
- performing, in said electronic circuit, content marking of said digital content based on said internally confined device-specific security data.

46. The method according to claim 45, wherein said step of performing content marking comprises the step of generating a device-specific fingerprint embedded into said digital content.

---